



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/603,209

06/25/2003

Ulrich Emmerling

071308.0443

2679

31625

7590

06/19/2006

BAKER BOTTS L.L.P.
PATENT DEPARTMENT
98 SAN JACINTO BLVD., SUITE 1500
AUSTIN, TX 78701-4039

EXAMINER

DWIVEDI, MAHESH H

ART UNIT

PAPER NUMBER

2168

DATE MAILED: 06/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/603,209

Applicant(s)

EMMERLING ET AL.

Examiner

Mahesh H. Dwivedi

Art Unit

2168

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 25 April 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-17 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-17 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 25 June 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 4/25/06.

- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Receipt of Applicant's Amendment, filed on 04/25/2006, is acknowledged. The amended parts include amended the specification, and amending claims 1-4, and 11-12.

Information Disclosure Statement

2. The information disclosure statements (IDS) submitted on 04/25/2006, 10/31/2005, and 10/28/2003 have been received, entered into the record, and considered. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statements are being considered by the examiner.

Specification

3. The objections raised in the office action mailed on 01/25/2006 have been overcome by the applicant's amendment received on 04/25/2006.

Claim Objections

4. The objections raised in the office action mailed on 01/25/2006 have been overcome by the applicant's amendment received on 04/25/2006.

Claim Rejections - 35 USC § 112

5. The objections raised in the office action mailed on 01/25/2006 have been overcome by the applicant's amendment received on 04/25/2006.

Claim Rejections - 35 USC § 102

Art Unit: 2168

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1-2, and 11 are rejected under 35 U.S.C. 102(e) as being anticipated by **Stellberger** (“Stellberger” (U.S. Patent 4,509,093)).

Regarding claim 1, **Stellberger** teaches a method comprising:

- a) transmitting an item of information unidirectionally between the first object and the at least one further object (Column 6, lines 60-67-Column 7, lines 1-8);
- b) calculating a computation result in the relevant receiving object from parts of the transmitted information (Column 7, lines 9-23);
- c) comparing the calculated computation result with a computation result transferred with the information in the relevant receiving object, (Column 4, lines 22-27, Column 9, lines 32-36); and
- d) authenticating the first object to the at least one further object only if there is a match between the calculated computation result and transferred computation result, and declaring the computation result as invalid for further transmissions (Column 5, lines 29-31).

The examiner notes that **Stellberger** teaches that the comparison phase can be performed on either the key or the lock. The examiner further notes that “The comparison phase between the output signals produced in each working cycle is

Art Unit: 2168

preferable made alternately in the key part and then in the lock part” (Column 4, lines 22-27) is analogous to “**comparing the calculated computation result with a computation result transferred with the information in the relevant receiving object**”. The examiner further notes that it is common knowledge that “random-access memory” (Column 5, lines 29-30) is refreshed after each cycle of inputting data. The examiner further notes that refreshing the data is analogous to declaring the data as “invalid”.

Regarding claim 2, **Stellberger** further teaches a method comprising:

- A) wherein the first object comprises a vehicle and the least further object comprises a key; and (Column 5, lines 58-61).
- B) wherein the information is transmitted from the vehicle and received by the key (Column 5, lines 58-61).

Regarding claim 11, **Stellberger** teaches a method comprising:

- a) transmitting an item of information unidirectionally between the vehicle and the key (Column 6, lines 60-67-Column 7, lines 1-8);
- b) calculating a computation result in the key from parts of the transmitted information (Column 7, lines 9-23);
- c) comparing the calculated computation result with a computation result transferred with the information, wherein the comparing is in the key (Column 4, lines 22-27, Column 9, lines 32-36); and

Art Unit: 2168

d) authenticating the vehicle if there is a match between the calculated computation result and the transferred computation result, and declaring the computation result as invalid for further transmissions (Column 5, lines 29-31).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Art Unit: 2168

9. Claims 3-10, and 12-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stellberger** (U.S. Patent 4,509,093) and in view of **Kocher et al.** (U.S. Patent 6,381,699).

10. Regarding claim 3, **Stellberger** teaches a method comprising:

A) a random number (Column 5, lines 29-31)

Stellberger, however, does not teach:

B) an incremental or decrementable item of data, wherein the incremental or decremental item of data is stored in the at least one further object if the calculated computation result matches the transferred computation result; and

C) wherein after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is transmitted (Kocher, Column 9, lines 23-45).

Kocher, however, teaches “an incremental or decrementable item of data, wherein the incremental or decremental item of data is stored in the at least one further object if the calculated computation result matches the transferred computation result” as “sends other needed information (such as data or t) to the verifier” (Column 9, lines 23-45), and “wherein after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is transmitted” as “if t matches, the verifier increments t” (Column 9, lines 23-45).

Art Unit: 2168

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher's** would have allowed **Stellberger's** provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claim 4, **Stellberger** teaches a method comprising:

A) a random number (Column 5, lines 29-31)

Stellberger, however, does not teach:

B) an incremental or decrementable item of data, wherein the incremental or decremental item of data is stored in the key if the calculated computation result matches the transferred computation result; and

C) wherein after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is transmitted (Kocher, Column 9, lines 23-45).

Kocher, however, teaches “an incremental or decrementable item of data, wherein the incremental or decremental item of data is stored in the key if the calculated computation result matches the transferred computation result” as “sends other needed information (such as data or t) to the verifier” (Column 9, lines 23-45), and “wherein after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new

Art Unit: 2168

information is transmitted” as “if t matches, the verifier increments t” (Column 9, lines 23-45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher’s** would have allowed **Stellberger’s** provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claims 5-6, and 13, **Stellberger** does not explicitly teach a method comprising:

A) wherein a counter state or item of time data is transferred as the item of data that can be incremented.

Kocher, however, teaches “a counter state or item of time data is transferred as the item of data that can be incremented” as “counter t” (Column 9, line 24).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher’s** would have allowed **Stellberger’s** provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claims 7 and 14, **Stellberger** does not explicitly teach a method comprising:

Art Unit: 2168

A) wherein the result is only calculated when the transferred item of data is greater than the stored item of data.

Kocher, however, teaches “**wherein the result is only calculated when the transferred item of data is greater than the stored item of data**” as “if the received value of t is larger than the internal value but the difference is not unreasonably large, it may be appropriate to accept the signature” (Column 9, lines 38-45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher’s** would have allowed **Stellberger’s** provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claims 8-9, and 15-16, **Stellberger** does not explicitly teach a method comprising:

A) wherein when the transferred result and the calculated result match, the incrementable item of data is increased so that the transferred result becomes invalid (Column 9, lines 23-45).

Kocher, however, teaches “**wherein when the transferred result and the calculated result match, the incrementable item of data is increased so that the transferred result becomes invalid**” as “if t matches” (Column 9, lines 38-45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching

Art Unit: 2168

Kocher's would have allowed **Stellberger's** provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claims 10 and 17, **Stellberger** does not explicitly teach a method comprising:

A) wherein the result is computed in at least one further object using a cryptological computation algorithm known there and a code word (Column 9, lines 8-22).

Kocher, however, teaches "a code word" as "symmetrically singed-code" (Column 9, line 10), and "**wherein the result is computed in at least one further object using a cryptological computation algorithm known there**" as "a hash or Mac of the data is typically computed using a secret key" (Column 9, lines 11-22).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher's** would have allowed **Stellberger's** provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claim 12, **Stellberger** teaches a method comprising:

A) a random number (Column 5, lines 29-31)

B) key (Column 5, lines 58-61)

Stellberger, however, does not teach:

Art Unit: 2168

B) an incremental or decrementable item of data, wherein the incremental or decremental item of data is stored in the key if the calculated computation result matches the transferred computation result; and

C) wherein after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is transmitted.

Kocher, however, teaches “an incremental or decrementable item of data which is stored in the key if it matches the computation result, is transferred” as “sends other needed information (such as data or t) to the verifier” (Column 9, lines 23-45), and “wherein after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is transmitted” as “if t matches, the verifier increments t” (Column 9, lines 23-45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching Kocher's would have allowed Stellberger's provide a system of security that remains secure even if attackers gather some information about the system, as noted by Kocher (Column 2, lines 40-44).

Response to Arguments

11. Applicant's arguments filed on 04/25/2006 have been fully considered but they are not persuasive.

Applicant suggests page 8 that **“Alternatively, in Stellberger the key always transmits the result of its calculation back to the lock unit because no comparison is performed in the key. Rather, the lock unit performs the comparison. Thus, Stellberger fails to teach the invention as claimed in claims 1 and 11”**. However, the examiner wishes to point to Column 4 of **Stellberger**, and refer to the second paragraph which states **“The comparison phase between the output signals produced in each working cycle is preferable made alternately in the key part and then in the lock part”** (Column 4, lines 22-27). The examiner wishes to state that **Stellberger’s** method includes having a comparison phase occurring either in the key or in the vehicle.

Applicant suggests page 9 that **“In Stellberger, the key always transmits the result calculation back to the lock unit because no comparison is performed in the key”**. However, the examiner wishes to point to Column 4 of **Stellberger**, and refer to the second paragraph which states **“The comparison phase between the output signals produced in each working cycle is preferable made alternately in the key part and then in the lock part”** (Column 4, lines 22-27). The examiner wishes to state that **Stellberger’s** method includes having a comparison phase occurring either in the key or in the vehicle.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. PGPUB 20010052075 issued to **Feinberg** on 13 December 2001. The subject matter disclosed therein is pertinent to that of claims 1-17 (e.g., methods to provide device authentication).

U.S. Patent 5,767,784 issued to **Khamhorn** on 16 June 1998. The subject matter disclosed therein is pertinent to that of claims 1-17 (e.g., methods to provide authentication for vehicle entry).

U.S. Patent 5,365,225 issued to **Bachhuber** on 15 November 1994. The subject matter disclosed therein is pertinent to that of claims 1-17 (e.g., methods to provide unidirectional authentication).

U.S. Patent 5,596,641 issued to **Ohashi et al.** on 21 January 1997. The subject matter disclosed therein is pertinent to that of claims 1-17 (e.g., methods to provide remote authentication).

U.S. Patent 4,935,962 issued to **Austin** on 19 June 1990. The subject matter disclosed therein is pertinent to that of claims 1-17 (e.g., methods to provide unidirectional authentication).

U.S. Patent 4,723,121 issued to **van den Boom et al.** on 02 February 1988. The subject matter disclosed therein is pertinent to that of claims 1-17 (e.g., methods to provide authentication for vehicle entry).

Art Unit: 2168

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Contact Information

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mahesh Dwivedi whose telephone number is (571) 272-2731. The examiner can normally be reached on Monday to Friday 8:20 am – 4:40 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tim Vo can be reached (571) 272-3642. The fax number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for

Art Unit: 2168

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should


you have questions on access to the Private PAIR system, contact the Electronic


Business Center (EBC) at 866-217-9197 (toll-free).

Mahesh Dwivedi

Patent Examiner

Art Unit 2168


June 5, 2006


Leslie Wong

Primary Examiner